УДК 681.3

БЛОКОВІ КРИПТОГРАФІЧНІ ПЕРЕТВОРЕННЯ З ВИКОРИСТАННЯМ ЛИШКОВИХ КЛАСІВ

Вячеслав Василенко
Відкрите акціонерне товариство "КП ОТІ"

Анотація: **Пропонується використання блокового криптографічного перетворення для задач забезпечення конфіденційності інформаційних об'єктів автоматизованих систем з використанням системи числення в лишкових класах.**
Summary: **The use of sectional cryptographic transformation for the tasks of providing of confidentiality of information's holding object of the automated systems with the use of scale of notation in remaining classes is offered.**
Ключові слова: **Інформація, конфіденційність, криптографічні перетворення, лишкові класи, системи числення.**

I Вступ

Однією із вкрай важливих для сучасних автоматизованих систем є проблема забезпечення конфіденційності та цілісності інформації [1 – 3], для вирішення якої застосовуються ті чи інші методи, методики чи алгоритми.

Для забезпечення конфіденційності інформації в багатьох випадках криптографічне перетворення є чи не єдиним шляхом забезпечення її конфіденційності (з певною стійкістю до спроб розкриття її змісту – криптографічною стійкістю). На цей час широко відомими є декілька алгоритмів криптографічного перетворення, із яких в Україні рекомендовано застосування алгоритму за ГОСТ 28147 – 89.

Слід звернути увагу на те, що одночасне забезпечення і конфіденційності і цілісності інформаційних об'єктів при використанні відомих алгоритмів досягається послідовним застосуванням процедур криптографічного перетворення і процедур обчислення цифрового підпису. При зворотному перетворенні спочатку перевіряється цілісність інформації, а потім здійснюється її дешифрування. Тобто цей процес є двофазним і при прямому і при зворотному перетворенні, за рахунок чого продуктивність засобів оброблення інформації дещо знижується.

Для усунення даного недоліку в [4] запропоновано низку кодових перетворень, в тому числі криптографічних із застосуванням процедур кодування шляхом перетворення з позиційної системи числення (ПСЧ) в систему лишкових класів (СЛК) та процедур декодування шляхом перетворення з системи лишкових класів в позиційну систему числення. В [4] показано також, що такі криптографічні перетворення (шифрування) вихідного тексту можна здійснити шляхом перемноження матриці – рядка, отриманої при представленні вихідного коду довжиною в k символів, і кодувальної матриці G (рис. 1) з k рядків і k стовпців. Правила вибору чи формування її елементів визначаються типом перетворення.

$$G = \begin{pmatrix} g_{11} & g_{12} & \cdot & g_{1n} & \cdot & g_{1k} \\ g_{21} & g_{22} & \cdot & g_{2n} & \cdot & g_{2k} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ g_{n1} & g_{n2} & \cdot & g_{nn} & \cdot & g_{nk} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ g_{k1} & g_{k2} & \cdot & \cdot & \cdot & g_{kk} \end{pmatrix}.$$

Рисунок 1 – Загальний вид кодувальної матриці

Код, отриманий у результаті множення вихідного коду на кодувальну матрицю, є деяким криптографічним перетворенням вихідного коду. Якщо механізм формування елементів кодувальної матриці є секретним, чи механізм формування елементів кодувальної матриці є загальновідомим, але при їхньому формуванні використовуються деякий секретний параметр – ключ, то зашифрований код має визначену криптографічну стійкість, тобто стійкість до спроб криптоаналітиків одержати з зашифрованого коду (часто з використанням певної частки відкритого вихідного тексту) ключ, чи власне вихідний код (текст). Така криптографічна стійкість є основною властивістю таких перетворень і досить часто визначається числом варіантів ключів.

У статті пропонуються методики отримання запропонованих в [4] матриць для прямих та зворотних перетворень з використанням лишкових класів та, як альтернатива, розглядаються кодові перетворення із

системи умовних лишків в позиційну, котрі, як показано нижче, є кращими від відомих.

II Методика побудови та застосування кодувальної матриці для блокового криптоперетворення типу – позиційна система числення → система лишкових класів

З урахуванням викладеного в [4], методика (алгоритм) блокового криптографічного перетворення вихідного m – символьного цифрового коду (блоку відкритого тексту з m символів), який вважається деяким числом А у позиційній системі числення (ПСЧ), в число Аслк в системі числення в лишкових класах (СЛК) зводиться до наступних процедур (операцій).

1. Представлення сукупності символів обраного позиційного представлення – вихідного слова для кодування у вигляді матриці – рядка розмірності ($l \times m$) виду $A = (a_1, a_2, ..., a_i, ..., a_m)$. З цією метою символи вихідного блоку слід розглядати як символи a_i $(i = 1, 2, ..., m)$ обраного позиційного представлення (цифри в позиційній системі числення числа A) з відповідними ваговими коефіцієнтами. Наприклад, для представлення в десятковій системі числення $c_i = 10i - 1$, для двійкового представлення при умові представлення символів вихідного коду, як байтів, $-ci = 256^{i-1}$. Неважко зрозуміти, що діапазон представлення таких чисел в першому випадку дорівнює $0 \le A < 10^m$, а в останньому $0 \le A < 256^m$;

2. Узгодження розмірів кодувальної матриці та вихідного слова для кодування. З цією метою необхідно:

– вибрати сукупність основ системи числення в залишкових класах з $n \ge m$ взаємно простих чисел p_j $(j = 1,2,...,n)$, p_j – j–та основа (елемент криптографічного ключа, за допомогою якого забезпечується потрібна криптографічна стійкість, див. далі). Кількість (n) основ p_j (основ, які утворюють діапазон представлення чисел в лишкових класах – "робочих" основ) слід обирати такою, щоб забезпечити умову $256^{m-1} \le P$, для двійкового представлення, чи $10^{i-1} \le P$. В останніх виразах $P = \prod_{j=1}^{n} p_j$, – діапазон представлення ("робочий" діапазон) СЛК.

Оскільки в подальшому постане питання про визначення елементів зворотної матриці, шляхом перетворення кодувальної матриці в декодувальну, яке є можливим лише для квадратних матриць, то, зрозуміло, що як розмірність для кодувальної матриці слід обирати більше із значень m та n. Позначимо розмірність кодувальної матриці k як $k = \max(m, n)$. Для узгодження розмірів матриць при $m < k$ вихідну матрицю $A = (a_1, a_2, ..., a_i, ..., a_m)$ слід доповнити $(s = k - m)$ нулями на місцях старших розрядних коефіцієнтів (як відомо при цьому величина чисел в ПСЧ не збільшується). При цьому вихідна матриця А набуде вигляду $A = (0, 0, ..., a_{s+1}, a_{s+2}, ..., a_{s+i}, ..., a_k)$, тобто замість розмірності ($l \times m$) отримає розмірність ($l \times k$).

– визначити розмірність кодувальної матриці як $(k \quad k)$, де $k = m + s$ чи $k = n + r$;

– визначити елементи g_{ij} кодувальної матриці G з розмірністю ($k \times k$)

$$g_{ij} = \{c_i\} p_j,$$

де знак $\{c_i\} p_j$ означає обчислення лишку (відрахування) від розподілу c_i на p_j;

3. Здійснення власне криптографічного перетворення $A_{СЛК} = A \times G$. При цьому слід враховувати, що всі операції мають здійснюватися за відповідними модулями, тобто при обчисленні першого елемента результуючої матриці – рядка – за модулем p_1, другого – за модулем p_2, i – го – за модулем p_i і т. ін.

Проілюструємо застосування цієї методики на наступних прикладах.

***Приклад* 1**. Застосування методики для умов прямого перетворення чисел із десяткової ПСЧ в систему лишкових класів (СЛК).

Нехай криптографічному перетворенню підлягає дворозрядне вихідне слово $A = 17$ $(m = 2)$ з

ваговими коефіцієнтами $c_1 = 10^0 = 1$ та $c_2 = 10^1 = 10$. У вигляді матриці – рядка це слово має вигляд $A = (1,7)$.

Виберемо сукупність основ системи числення в залишкових класах. Нехай це є основи $p_1 = 2,\ p_2 = 3,\ p_3 = 5\ (n = 3)$. Тоді діапазон представлення чисел ("робочий" діапазон) в СЛК $P = \prod_{j=1}^{j=3} p_j = 30$.

Визначимо розмірність кодувальної матриці k як $k = \max(m,n) = 3$. Для узгодження розмірів матриць ($m < k$) вихідну матрицю $A = (a_1, a_2, a_3)$ слід доповнити одним $(s = k - m = 1)$ нулем на місці старшого розрядного коефіцієнту. При цьому вихідна матриця A набуде вигляду $A = (0, a_2, a_3) = (0\ 1\ 7)$ з ваговими коефіцієнтами $c_1 = 10^0 = 1,\ c_2 = 10^1 = 10$ та $c_3 = 10^2 = 100$, тобто замість розмірності ($l \times 2$) отримає розмірність ($l \times 3$).

Створимо кодувальну матрицю G з розмірністю (3×3), елементами g_{ij} якої використаємо величини $g_{ij} = \{c_i\}p_j$, де знак $\{c_i\}p_j$ означає обчислення залишку (відрахування) від розподілу c_i на p_j. В результаті отримаємо $g_{11} = \{100\}_2 = 0,\ g_{12} = \{100\}_3 = 1,\ g_{13} = \{100\}_5 = 0,\ g_{21} = \{10\}_2 = 0,\ g_{22} = \{10\}_3 = 1,\ g_{23} = \{10\}_5 = 0,\ g_{31} = \{1\}_2 = 1,\ g_{32} = \{1\}_3 = 1,\ g_{33} = \{1\}_5 = 1,$ тобто:

$$G = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}.$$

Здійснимо перетворення

$$A_{слк} = A \times G = (0, 1, 7) \times \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} = (1, 2, 2).$$

Неважко переконатися в правильності виконаного перетворення.

***Приклад* 2**. Застосування методики для умов прямого перетворення чисел із десяткової ПСЧ в систему лишкових класів (СЛК) для іншої сукупності основ системи числення в залишкових класах. Нехай це є основи $p_1 = 3,\ p_2 = 7,\ p_3 = 11$ (n = 3). Тоді діапазон представлення чисел ("робочий" діапазон) в СЛК $P = \prod_{j=1}^{j=3} p_j = 231$.

1. Визначимо розмірність кодувальної матриці k. Як і в попередньому прикладі k = max (m,n) = 3. При цьому вихідна матриця A, як і раніше, має вигляд $A = (0, a_2, a_3) = (0, 1, 7)$ з ваговими коефіцієнтами $c_1 = 10^0 = 1$, $c_2 = 10$ та $c_3 = 100$, тобто має розмірність (1×3).

2. Створимо кодувальну матрицю G з розмірністю (3×3). В результаті отримаємо $g_{11} = \{100\}_3 = 1$, $g_{12} = \{100\}_7 = 2$, $g_{13} = \{100\}_{11} = 1$, $g_{21} = \{10\}_3 = 1$, $g_{22} = \{10\}_7 = 3$, $g_{23} = \{10\}_{11} = 10$, $g_{31} = \{1\}_3 = 1$, $g_{32} = \{1\}_7 = 1$, $g_{33} = \{1\}_{11} = 1$, тобто:

$$G = \begin{pmatrix} 1 & 2 & 1 \\ 1 & 3 & 10 \\ 1 & 1 & 1 \end{pmatrix}.$$

3. Здійснимо перетворення

$$A_{слк} = A \times G = (0, 1, 7) \times \begin{pmatrix} 1 & 2 & 1 \\ 1 & 3 & 10 \\ 1 & 1 & 1 \end{pmatrix} = (2, 3, 6).$$

Неважко переконатися в правильності виконаного перетворення.

Таким чином, наведені ілюстративні приклади підтверджують правильність запропонованої методики побудови та застосування кодувальних матриць для блокового криптоперетворення типу – позиційна

система числення → система лишкових класів.

III Методики побудови декодувальних матриць для дешифрування (зворотного криптоперетворення) блокового криптоперетворення типу – система лишкових класів → позиційна система числення

Для зворотного перетворення необхідно:

1. визначити елементи зворотної матриці G^{-1};
2. здійснити зворотне перетворення $A = A_{слк} \times G^{-1}$.

Для зрозуміння подальших міркувань щодо зворотного перетворення чисел із СЛК в ПСЧ розглянемо процедури визначення елементів зворотної матриці G^{-1} для розглянутих вище прикладів прямого перетворення із позиційної десяткової системи числення (ПСЧ) в систему лишкових класів (СЛК).

При визначенні елементів зворотної матриці G^{-1} нагадаємо, що така (зворотна) матриця існує, якщо детермінант для прямої матриці G є відмінним від нуля, тобто $\det G \neq 0$.

Приклад 3. Спробуємо отримати зворотну матрицю для перетворення СЛК → ПСЧ для умов прямого перетворення за прикладом 1. Не важко переконатися, що для цього прикладу, нажаль, $\det G = 0$, тобто отримати зворотну матрицю G^{-1} традиційним математичним методом неможливо. Це пояснюється тим, що в матриці G є однаковими перший та другий рядки, а також перший та третій стовпчики, коли за властивостями детермінанту він дорівнює нулю. Останнє, в свою чергу, є наслідком того, що основи $p_1 = 2$ та $p_3 = 5$ є дільниками усіх вагових розрядів ПСЧ. Але аналогічна ситуація може бути і в випадку, коли основами СЛК будуть обрані числа, величина яких перевищує значення вагових коефіцієнтів (наприклад, $c_1 = 10^0 = 1$, $c_2 = 10^1 = 10$, ...). Тоді в кодувальній матриці з'являться рядки, які є лінійними комбінаціями один одного, внаслідок чого за властивостями детермінанту він буде дорівнювати нулю.

Примітка 1. Таке явище призводить до зменшення кількості чисел, які можуть бути використаними як основи СЛК і, зрозуміло, – до зменшення кількості варіантів ключів, що має своїм наслідком зниження криптографічної стійкості коду.

Першим способом уникнення цього ускладнення є вибір таких основ, які не є дільниками вагових розрядів. Для ілюстрації цього підходу розглянемо наступний приклад для умов перетворення того ж самого вихідного слова A = (1,7) із тими ж, зрозуміло, ваговими коефіцієнтами $c_1 = 1$ та $c_2 = 10$.

Приклад 4. Визначимо елементи зворотної матриці G^{-1} для умов прямого перетворення за прикладом 2. Для цього спочатку перевіримо, що вона існує. Дійсно, для заданих умов $\det G = 9 \neq 0$, тобто зворотна матриця існує. Не важко переконатися, що така матриця має вигляд

$$G^{-1} = (1/9) \begin{pmatrix} -7 & -1 & 17 \\ 9 & 0 & -9 \\ -2 & 1 & 1 \end{pmatrix}.$$

На розвиток цього прикладу і для перевірки правильності отримання зворотної матриці розглянемо приклади перетворення кодів із СЛК в ПСЧ.

***Приклад* 4.1.** Нехай перше число в СЛК є $A_{слк} = (1, 1, 1)$. Тоді

$$A_{ПСЧ} = A_{слк} \times G^{-1} = (1, 1, 1) \times (1/9) \begin{pmatrix} -7 & -1 & 17 \\ 9 & 0 & -9 \\ -2 & 1 & 1 \end{pmatrix} = (1/9)\,(0, 0, 9) = (0, 0, 1) = 1.$$

Неважко переконатися в правильності виконаного перетворення.

***Приклад* 4.2.** Нехай другим числом в СЛК є $A_{слк} = (0, 3, 3)$. Тоді

$$A_{ПСЧ} = A_{слк} \times G^{-1} = (0, 3, 3) \times (1/9) \begin{pmatrix} -7 & -1 & 17 \\ 9 & 0 & -9 \\ -2 & 1 & 1 \end{pmatrix} = (1/9)\,(21, 3, -24).$$

Такий вигляд отриманого числа в ПСЧ є досить незвичним. Але його легко перетворити у звичний вигляд, якщо згадати, що при записі чисел в поліноміальній формі слід писати

$$A_{ПСЧ} = (1/9)\,(21, 3, -24) = (1/9)\,(21 \circledcirc 100 + 3 \circledcirc 10 + (-24) \circledcirc 1) = (1/9) \circledcirc 2106 = 234.$$

Звернемо увагу також на те, що отриманий результат перевищує допустиме значення, тобто число $A_{ПСЧ}$ вийшло за межі робочого діапазону СЛК: $A_{ПСЧ} = 234 > 231$. Для вводу цього числа в робочий діапазон слід здійснити операцію $A_{ПСЧ} = \{ A_{ПСЧ} \}_{231} = \{ 234 \}_{231} = 3$. Неважко переконатися в правильності виконаного перетворення.

Звернемо увагу на те, що останні перетворення пов'язані з наступними властивостями.

Запис чисел в ПСЧ є формою їх скороченого поліноміального представлення

$$A_{ПСЧ} = a_{n-1} \odot 10^{n-1} + a_{n-2} \odot 10^{n-2} + \ldots + a_2 \odot 10^{2} + a_1 \odot 10^{1} + a_0 \odot 10^{0}. \quad (1)$$

Величина чисел в ПСЧ, отриманих внаслідок усіх перетворень, не повинна перевищувати діапазон їх представлення в СЛК $P = \prod_{j=1}^{j=n} p_j$.

При представленні чисел в ПСЧ слід враховувати наявність міжрозрядних зв'язків та можливості запозичення із старших розрядів в молодші та переносів із молодших розрядів в старші в разі, коли значення розрядних коефіцієнтів:

а) є меншими за нуль;

б) є більшими за 10.

Це призводить до того, що результат перетворення в останній ілюстрації у вигляді

$$A_{ПСЧ} = (1/9)\ (21, 3, -24)$$

слід послідовно записати у вигляді

$$A_{ПСЧ} = (1/9)\ (21, 3, --24) = (1/9)\ (21, 0, 6) = (1/9)\ (2, 1, 0, 6),$$

по-перше, як наслідок запозичення із другого розряду трьох десятків для отримання невід'ємного значення першого розрядного коефіцієнта, та, по-друге, переносу двох десятків із третього розрядного коефіцієнта як двох одиниць до четвертого розрядного коефіцієнта.

Внаслідок реалізації перших трьох властивостей операцію ділення на детермінант слід здійснювати по відношенню до єдиного десяткового числа в формі (1), отримавши при цьому $A_{ПСЧ} = 2106/9 = 234$, та $A_{ПСЧ} = \{234\}_{231} = 3$.

Такі ж наслідки можна отримати, здійснивши операції за п. 3 щодо елементів декодувальної матриці, звернувши увагу на те, що результат множення вектора – рядка $A_{слк}$ на зворотну матрицю G^{-1} можна записати у вигляді

$$A_{ПСЧ} = A_{слк} \times G^{-1} = (0, 3, 3) \times (1/9) \begin{pmatrix} -7 & -1 & 17 \\ 9 & 0 & -9 \\ -2 & 1 & 1 \end{pmatrix} =$$

$$= (1/9)\ [(0 \odot (-7) + 3 \odot 9 + 3 \odot (-2)), (0 \odot (-1) + 3 \odot 0 + 3 \odot 1), (0 \odot 17 + 3 \odot (-9) + 3 \odot 1)],$$

де в кожній із круглих дужок записані результати обчислення вагових коефіцієнтів ПСЧ.

Тоді

$$A_{ПСЧ} = (1/9)\ [(0 \odot (-7) + 3 \odot 9 + 3 \odot (-2)), (0 \odot (-1) + 3 \odot 0 + 3 \odot 1), (0 \odot 17 + 3 \odot (-9) + 3 \odot 1)],$$

після врахування вагових коефіцієнтів

$$A_{ПСЧ} = (1/9)\ [(0 \odot (-7) + 3 \odot 9 + 3 \odot (-2)) \odot 100 + (0 \odot (-1) + 3 \odot 0 + 3 \odot 1) \odot 10 + (0 \odot 17 + 3 \odot (-9) + 3 \odot 1) \odot 1],$$

групування щодо елементів матриці – рядка

$$A_{ПСЧ} = (1/9)\ \{0 \odot [(-7) \odot 100 + (-1) \odot 10 + 17 \odot 1] + 3 \odot [9 \odot 100 + 0 \odot 10 + (-9) \odot 1] + 3 \odot [(-2) \odot 100 + 1 \odot 10 + 1 \odot 1]\} = (1/9)\ [0 \odot (-700 - 10 + 17) + 3 \odot (900 - 9) + 3 \odot (-200 + 10 + 1)] = (1/9)\ [0 \odot (-693) + 3 \odot 891 + 3 \odot (-189)],$$

та ділення на величину детермінанта отримаємо

$$A_{ПСЧ} = 0 \odot (-77) + 3 \odot 99 + 3 \odot (-21).$$

Для позбавлення від від'ємних величин введемо результати обчислення в межі робочого діапазону

$$A = \{A_{ПСЧ}\}_P = \{\{0 \odot (-77)\}_P + \{3 \odot 99\}_P + 3 \odot \{(-21)\}_P\}_P = \{\{0 \odot (-77 + 231) + \{3 \odot 99\}_P + \{3 \odot (-21 + 231)\}_P\}_P = \{\{0 \odot 154 + \{3 \odot 99\}_P + \{3 \odot 210\}_P\}_P = \{0 + 66 + 168\}_P = \{234\}_P = 3.$$

Такий довгий шлях достатньо елементарних розрахунків ми зробили лише для того, щоб звернути увагу на проміжний результат останнього розрахунку у вигляді

$$\{A_{ПСЧ}\}_P = \{\{0 \odot 154 + \{3 \odot 99\}_P + \{3 \odot 210\}_P\}_P,$$

що можна трактувати як результат операції

$$A_{ПСЧ} = A_{слк} \times G^{-1} = (0, 3, 3) \times \begin{pmatrix} 1 & 5 & 4 \\ 0 & 9 & 9 \\ 2 & 1 & 0 \end{pmatrix} = \{6 \odot 100 + 30 \odot 10 + 27\}_P = \{927\}_{231} = 3.$$

1. Звернемо увагу також, що до зворотної матриці G^{-1} у вигляді

$$G^{-1} = \begin{pmatrix} 1 & 5 & 4 \\ 0 & 9 & 9 \\ 2 & 1 & 0 \end{pmatrix}$$

можна прийти шляхом низки наступних перетворень

$$G^{-1} = (1/9)\begin{pmatrix} -7 & -1 & 17 \\ 9 & 0 & -9 \\ -2 & 1 & 1 \end{pmatrix} = (1/9)\begin{pmatrix} -7 & 0 & 7 \\ 8 & 9 & 1 \\ -2 & 1 & 1 \end{pmatrix} = (1/9)$$

$$\begin{pmatrix} -693 \\ 891 \\ -189 \end{pmatrix} = \begin{pmatrix} -077 \\ 099 \\ -021 \end{pmatrix} = \begin{pmatrix} -077 \\ 099 \\ -021 \end{pmatrix} + \begin{pmatrix} 2 & 3 & 1 \\ 0 & 0 & 0 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 5 & 4 \\ 0 & 9 & 9 \\ 2 & 1 & 0 \end{pmatrix}.$$

В цій низці перетворень використані операції міжрозрядних запозичень та переносів, а також операції введення результатів в межі робочого діапазону.

8. І, нарешті, покажемо, що ця матриця є не що інше, як, розклад по елементах матриці ортогональних базисів з обраними основами системи числення в лишкових класах. Дійсно, для обраного набору основ $p_1 = 3$, $p_2 = 7$, $p_3 = 11$ (n = 3) з діапазоном представлення чисел ("робочим" діапазоном) $P = \prod_{j=1}^{j=3} p_j = 231$, константами $P_1 = 231/3 = 77$, $P_2 = 231/7 = 33$, $P_3 = 231/11 = 21$, маємо "ваги" ортогональних базисів системи $m_1 = 2$, $m_2 = 3$, $m_3 = 10$, що дає значення ортогональних базисів системи $B_1 = 154$, $B_2 = 099$, $B_3 = 210$.

Таким чином, елементи матриці для зворотного перетворення із СЛК в ПСЧ можна визначати шляхом класичних математичних перетворень лише в окремих випадках. Більш універсальним є визначення таких матриць, виходячи із властивостей коду, тобто як значення ортогональних базисів системи. Останнє було визначено в [4, 5] при розгляді питання про завадостійкі перетворення, коли як зворотну матрицю G^{-1} запропоновано використати спрощену зворотну матрицю виду

$$G^{-1} = \begin{pmatrix} g_{11} & B_{21} \\ g_{12} & B_{22} \\ . & . \\ g_{1k} & B_{2k} \end{pmatrix}.$$

Такий підхід розв'язує проблему щодо визначення матриць для декодування (для зворотного перетворення із СЛК в ПСЧ) у разі коли детермінант кодувальної матриці дорівнює нулю. Тим самим знімаються і обмеження з вибору основ СЛК і, отже, обмеження щодо криптографічної стійкості коду (див. примітку 1).

IV Методики блокових криптоперетворень типу система лишкових класів → позиційна система числення

Уважне ознайомлення з отриманими в попередніх розділах результатами дає можливість стверджувати, що перетворення із ПСЧ в СЛК є можливим для будь-якої сукупності основ, які задовольняють відповідним вимогам. Таким чином, розглянуті методики дозволяють здійснити блокові криптоперетворення типу – позиційна система числення → система лишкових класів із певною криптографічною стійкістю. Однак такі перетворення мають і певні вади, до яких можна віднести:

1. недостатню криптографічну стійкість, пов'язану з можливістю розкриття шифру, тобто визначення величин основ СЛК при достатньо тривалому спостереженні за блоками закритого тексту; це є можливим завдяки тому, що максимальне значення лишків за певною основою p_i дорівнює $(p_i - 1)$, тобто визначення при тривалому спостереженні величини $(p_i - 1)$, однозначно визначає і p_i; можна запропонувати способи запобігання цьому, але вони пов'язані з необхідністю додаткових операцій при перетворенні в СЛК;

2. велику надлишковість закритого тексту порівняно з відкритим; останнє пояснюється тим, що збільшення криптографічної стійкості коду є можливим за рахунок використання значної кількості основ – взаємно простих чисел, величини яких перевищують (а при їх великій кількості – значно перевищують) величину основи в ПСЧ; тобто, якщо вихідний код потребує для запису (передавання, збереження та ін.) g розрядів, то кожен символ зашифрованого тексту – не менше ніж (g + 1). Це, в свою чергу, призводить або до необхідності використання при запису кожного із символів СЛК подвійної розрядності (порівняно с символами ПСЧ), або ж до необхідності здійснювати "переупаковку" зашифрованого тексту з метою його ущільнення (із зворотною процедурою розущільнення), що вимагає значних затрат обчислювальних ресурсів.

Тому, як альтернатива розглянутим методикам перетворень із позиційних систем в систему лишкових класів пропонуються методики криптографічних перетворень за схемами: при шифруванні – перетворення із системи лишкових класів в позиційну систему числення, при дешифруванні – перетворення із позиційної системи числення в систему лишкових класів. З цією метою будемо уявляти усі символи вихідного блока для шифрування

$$A = \alpha_1, \alpha_2, \ldots, \alpha_k,$$

незалежно від початкової системи числення (для визначеності в межах статті початкова система числення нехай буде позиційною), символами в деякій ***умовній СЛК*** – лишками за основами p_i (i = 1, 2, ..., k). Щоб символи початкової системи числення можна було вважати символами в умовній СЛК, значення основ цієї умовної СЛК p_i слід вибирати з умови

$$p_i > g^f,$$

де g – основа вихідної системи числення, а f – розрядність символів початкової системи числення. Ця вимога пов'язана з тим, що в СЛК значення основ є завжди більшими, ніж значення лишків за цими основами (а це – значення символів початкової системи числення).

Методику блокових криптоперетворень типу система лишкових класів → позиційна система числення проілюструємо, як і раніше, конкретними прикладами.

***Приклад* 5.** Нехай криптографічному перетворенню підлягає дворозрядне вихідне слово A = 17 (m = 2) в десятковій системі числення. Тоді g = 10, а f = 1. Вважаємо, що це число є число в умовній СЛК $A_{слк}$ = (1, 7). Визначимо основи цієї умовної СЛК. Нехай такими основами будуть p_1 = 11, та p_2 = 13. При цьому P_1 = 13, P_2 = 11, m_1 = 6, m_2 = 6, B_1 = 78, B_2 = 66. Тоді, з урахуванням попередніх результатів, кодуючу та декодуючу матриці слід записати у вигляді

$$G = \begin{pmatrix} 7 & 6 \\ 8 & 6 \end{pmatrix}, G^{-1} = \begin{pmatrix} 1 & 9 \\ 10 & 10 \\ 1 & 1 \end{pmatrix},$$

перетворене (зашифроване) в ПСЧ число

$$A_{псч} = (1, 7) \times \begin{pmatrix} 7 & 6 \\ 8 & 6 \end{pmatrix} = (63, 48) = (111),$$

а дешифроване –

$$A = (111) \times \begin{pmatrix} 1 & 9 \\ 10 & 10 \\ 1 & 1 \end{pmatrix} = (\{12\}_{11}, \{20\}_{13}) = (1, 7),$$

що відповідає вихідному числу 17, яке підлягало прямому (в ПСЧ) та зворотному (в умовну СЛК) перетворенням.

Неважко упевнитися, що криптографічне перетворення за такою схемою є вільним від викладених вище вад, оскільки представлення зашифрованого тексту в позиційній (особливо в двійковій) системі числення має, внаслідок властивостей ПСЧ, найвищу щільність упаковки. При цьому задачі ущільнення та розущільнення є зайвими; оскільки зашифрований текст представляється в позиційній системі числення, то розкрити шифр, тобто набір основ в умовній СЛК, шляхом статистичного аналізу величин символів, є неможливим (скоріше за все для цього потрібен лише прямий перебір усіх їх можливих варіантів).

Таким чином, варіант блокових криптоперетворень типу – умовна система лишкових класів → позиційна система числення, порівняно із запропонованим в [4] варіантом криптоперетворень типу позиційна система → система числення лишкових класів, є більш досконалим.

*Література: **1.** Нормативний документ Системи технічного захисту інформації "Загальні положення про захист інформації в комп'ютерних системах від несанкціонованого доступу" (НД ТЗІ 1.1-002-99). **2**. Нормативний документ Системи технічного захисту інформації "Критерії оцінки захищеності інформації в комп'ютерних системах від НСД" (НД ТЗІ 2.5-004-99). **3**. Нормативний документ Системи технічного захисту інформації "Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу" [НД ТЗІ 2.5-005-99]. **4**. Василенко В. С. Варіант завадостійкого криптографічного перетворення // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 8, 2004 р. – с. 101 – 108.*